

**EXPRESS MAIL LABEL NO.: EL563155563US**

**DATE MAILED:** September 6, 2000

**PATENT**

**INVENTOR:** William A. Chren, Jr.

**RESIDUE NUMBER SYSTEM ARITHMETIC CIRCUITS  
WITH BUILT-IN SELF TEST**

5

**BACKGROUND OF THE INVENTION**

**1. Field of the Invention**

The present invention relates to electronic circuits, and more specifically to arithmetic circuits having built-in self testing for use with the residue number system.

10

**2. Description of Related Art**

Power consumption is now a very important consideration in integrated circuit design. This has compelled circuit designers to consider reducing power consumption through changes in many different levels of the design process, such as the system, technology, algorithm, physical, and circuit levels. For example, system level approaches for reducing power consumption include power supply voltage scaling, clock gating, and subsystem sleep (or power down) modes. Technology level techniques include using dynamic threshold MOSFETs, and algorithm level techniques include using alternate number systems and state encoding. Further, physical level methods include transistor reordering, and circuit level methods include self-timed asynchronous approaches and glitch reduction. The ultra-low power circuits of the future will have to employ several of these approaches because none alone can achieve the power reduction goals for the next decade.

15

20

While all of the techniques described above advantageously reduce power consumption, many of them have a deleterious side effect of reducing the speed of the circuit. For example, supply voltage scaling lengthens the system clock period if other

25

**EXPRESS MAIL LABEL NO.: EL563155563US**

factors such as technology and drive strength are kept the same. For this reason, designers now consider the delay-power (DP) product of a circuit as the crucial factor in low power circuit design. One system level design approach that is currently being investigated due to of its potential for significantly reducing the DP product is the One-  
5 Hot Residue Number System (OHRNS). For example, the OHRNS is being considered for use in the adaptive FIR (finite impulse response) filters and Viterbi detectors of hard disk drive read channels, in the endecs of wireless telecommunication integrated circuits, and in the adaptive filters of image processing integrated circuits.

10 The Residue Number System (RNS) is an integer number system in which the basic operations of addition, subtraction, and multiplication can be performed quickly because there are no carries, borrows, or partial products. This allows the basic operations to be performed in a single combinational step, digit-on-digit, using simple arithmetic units operating in parallel. However, other operations such as magnitude comparison, scaling (the RNS equivalent of right shifting), base extension (the RNS  
15 equivalent of increasing the bit width), and division are slower and more complicated to implement. Thus, RNS is most widely used in applications in which the basic operations predominate, such as digital signal processing.

The RNS representation of an integer  $X$  is a number of digits, with each digit being the residue of  $X$  modulo a specially chosen integer modulus. In other words,  $X$  is  
20 represented as the vector of its residues modulo a fixed set of integer moduli. In order to make the RNS representation of each integer unique for all non-negative values less than the product  $M$  of the moduli, the moduli are chosen to be pairwise relatively prime (i.e., the smallest single number into which all divide evenly is equal to the product of the moduli). Letting  $m_i$  denote the  $i^{\text{th}}$  modulus, the RNS representation of  $X$  is given by  
25  $X \rightsquigarrow (x_1, x_2, \dots, x_n)$ , where  $x_j = X \text{ modulo } m_j$  and is known as the  $i^{\text{th}}$  residue digit of the RNS representation of  $X$ . Table 1 shows the representation of the integers 0 to 2430 in an RNS in which  $m_1=11$ ,  $m_2=13$ , and  $m_3=17$  ("an 11, 13, 17 RNS representation").

EXPRESS MAIL LABEL NO.: EL563155563US

TABLE 1

Integer X	RNS digit $x_{11}$	RNS digit $x_{13}$	RNS digit $x_{17}$
2430	10	12	16
2429	9	11	15
...			
19	8	6	2
18	7	5	1
17	6	4	0
16	5	3	16
15	4	2	15
14	3	1	14
13	2	0	13
12	1	12	12
11	0	11	11
10	10	10	10
9	9	9	9
8	8	8	8
7	7	7	7
6	6	6	6
5	5	5	5
4	4	4	4
3	3	3	3
2	2	2	2
1	1	1	1
0	0	0	0

As an example, for the natural number 19, the  $x_{11}$  digit is  $19 \bmod(11) = 8$  (i.e.,

$19 \div 11 = 1$  remainder 8), the  $x_{13}$  digit is  $19 \bmod(13) = 6$ , and the  $x_{17}$  digit is

$19 \bmod(17) = 2$ . Each RNS digit is determined without reference to any other

RNS digit, and no RNS representation repeats in the range from 0 to 2430. Negative

integers can be represented by limiting the represented range to an equal (or substantially

**EXPRESS MAIL LABEL NO.: EL563155563US**

equal) number of positive and negative numbers. The representation of the range from -1215 to 1215 in the 11, 13, 17 RNS representation is shown in Table 2. No separate sign is associated with the RNS representation, and the sign of the represented integer cannot be determined from any less than all of its RNS digits.

5

TABLE 2

Integer X	RNS digit $x_{11}$	RNS digit $x_{13}$	RNS digit $x_{17}$
1215	5	6	8
1214	4	5	7
...			
4	4	4	4
3	3	3	3
2	2	2	2
1	1	1	1
0	0	0	0
-1	10	12	16
-2	9	11	15
-3	8	10	14
-4	7	9	13
...			
-1214	7	8	10
-1215	6	7	9

25

In the RNS, the basic operations of addition, subtraction, and multiplication are performed in digit-parallel fashion, modulo  $m_i$ . Thus, if operands X and Y have RNS representations of  $X \leftrightarrow (x_1, x_2, \dots, x_n)$  and  $Y \leftrightarrow (y_1, y_2, \dots, y_n)$ , the result Z has an RNS representation of  $Z \leftrightarrow (x_1 \circ y_1, x_2 \circ y_2, \dots, x_n \circ y_n)$ , where " $x_i \circ y_i$ " represents any of the basic operations performed on the two RNS digits modulo  $m_i$ . More specifically, the corresponding RNS digits of the two numbers are added, subtracted, or multiplied, and

30

**EXPRESS MAIL LABEL NO.: EL563155563US**

then the proper modulo operation is performed on each to produce the RNS digits of the result.

For example, in the 11, 13, 17 RNS representation of Table 1,  $4+15$  gives  $(4, 4, 4) + (4, 2, 15)$  or  $(4+4 \bmod(11), 4+2 \bmod(13), 4+15 \bmod(17))$ , which equals  $(8, 6, 2)$  or 19. Similarly,  $19-15$  gives  $(8-4 \bmod(11), 6-2 \bmod(13), 2-15 \bmod(17))$ , which equals  $(4, 4, 4)$  or 4. Further,  $6 \times 3$  gives  $(6 \times 3 \bmod(11), 6 \times 3 \bmod(13), 6 \times 3 \bmod(17))$ , which equals  $(7, 5, 1)$  or 18. Because all individual operations are performed on each RNS digit independently and without reference to any other RNS digit, the operations can be performed completely in parallel. Thus, each of the basic operations can be performed quickly and efficiently, especially when all of the moduli are relatively small integers.

In electronic circuit implementations, addition is the fundamental RNS operation and subtraction is performed by adding the additive inverse of the subtrahend. Multiplication is also performed using addition by using of the following properties. Any prime modulus  $p$  has at least one primitive root, which is an integer  $\alpha$  of order  $p-1$  under multiplication. In other words, the primitive root is an integer  $\alpha$  whose successive powers, taken modulo  $p$ , are the nonzero integers modulo  $p$  (i.e., for any  $0 \leq X < p$ ,  $X = \alpha^k \bmod p$  for some  $0 \leq k \leq p-2$ ). In such a case,  $X$  is said to have an index of  $k$ , modulo  $p$ .

Given the primitive root, multiplication modulo  $p$  can be performed by adding the indices modulo  $p-1$ . This is analogous to using logarithms in the binary number system. For example,  $\alpha = 2$  is a primitive root modulo 13 because, the integers  $2^0, 2^1, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8, 2^9, 2^{10}$ , and  $2^{11}$  modulo 13 are equal to 1, 2, 4, 8, 3, 6, 12, 11, 9, 5, 10 and 7, respectively. Thus, if  $X=5$  ( $2^9$  modulo 13) and  $Y=7$  ( $2^{11}$  modulo 13),  $X \times Y = 35$  ( $2^8$  modulo 13). Thus, the index of the product modulo  $p$  (8) of two RNS digits can be determined by adding the indices of the two RNS digits (9 and 11), modulo  $p-1$  (i.e.,  $(9+11) \bmod(12) = 8$ ).

**EXPRESS MAIL LABEL NO.: EL563155563US**

In electronic circuit implementations, the RNS digits can be encoded in various ways. In conventional binary encoding, each RNS digit is converted to a binary number that is represented by the states of one or more lines, each of which is in one of two states to represent a binary digit of "0" or "1". There is also the "one-hot" encoding scheme in which each possible value of an RNS digit is associated with a separate two-state line. For example, in the 11, 13, 17 RNS representation, 11 lines are used to represent the first RNS digit, 13 lines are used to represent the second RNS digit, and 17 lines are used to represent the third RNS digit. When an RNS digit has a given value, the line associated with that value is high and all of the other lines are low. Thus, only one line of a digit is high (or hot) at any given time.

The use of the one-hot encoding scheme with the RNS produces such compelling advantages in electronic circuit implementations that such a system is identified as the "One-Hot Residue Number System" (OHRNS). While the OHRNS is really the same RNS with the same arithmetic properties, the advantages of using one-hot encoding include basic operation implementation using barrel shifters with their superior delay-power products and operand-independent delays, simple and regular layout of arithmetic circuits, and zero-cost implementation through signal transposition of inverse calculation, index calculation, and residue conversion. When any RNS digit changes in value, at most two lines change state. This is the minimal possible activity factor and yields low power dissipation. Because in OHRNS implementations signal activity factors are near minimal and fewer critical path transistors are present, such systems have very low delay-power products. (A detailed explanation of OHRNS circuits can be found in W.A. Chren, Jr., "One-Hot Residue Coding for Low Delay-Power Product CMOS Design," IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing, v. 45, no. 3 (March 1998), pp. 303-313, which is herein incorporated by reference.)

With one-hot encoding of the RNS digits, addition can be performed through a cyclic shift (i.e., rotation). In particular, one of the operands is rotated by an amount

**EXPRESS MAIL LABEL NO.: EL563155563US**

equal to the value of the other operand. While such a rotation can be implemented using several different types of circuits, barrel shifters allow all possible rotations of the first operand to be computed in parallel. The second operand determines which of the rotations is output from the barrel shifter as the result. A conventional OHRNS modulo  $m_i$  adder is shown in Figure 1(a). The adder 10 includes a modulo  $m_i$  barrel shifter 12 that performs the addition, and a static pipeline register 14 that stores the result for downstream processing. Figure 1(b) shows the internal structure of the barrel shifter. As shown, NMOS pass transistors 16 are used instead of transmission gates to yield higher speed and lower power dissipation due to smaller input and output capacitive loadings (i.e., because there are half as many NMOS sources/drains per input/output line as when transmission gates are used).

Further, in the OHRNS, subtraction can be performed by adding the additive inverse of the subtrahend, and the additive inverse can be computed by a simple one-to-one mapping using signal transposition. Figure 2 shows a conventional OHRNS modulo  $m_i$  subtractor. As shown, the subtractor 20 is identical to the adder 10 of Figure 1(a) except for the use of signal transposition 22 on the subtrahend input to the barrel shifter 12. The signal transposition 22 computes the additive inverse quickly and simply through a one-to-one mapping of inputs to outputs.

Multiplication in the OHRNS can also be performed with barrel shifters by using indices. Indices and their additive inverses, which are known as anti-indices, are the RNS equivalents of logarithms and antilogarithms, as explained above. The computation of indices and anti-indices in any modulus can be performed quickly and simply through a one-to-one mapping. In particular, such mappings in the OHRNS are implemented by merely permutating the signal lines of the RNS digit. In other words, indices and anti-indices can be computed through signal transpositions or wire permutations that require no active circuitry and introduce little or no delay.

Figure 3 shows a conventional OHRNS modulo  $m_i$  multiplier that uses wire transpositions to compute indices and anti-indices. More specifically, the multiplier 30 uses signal transpositions 34, 36, and 38 on the input and output lines to compute the indices and anti-indices, and a barrel shifter 32 to add the indices. A small amount of combinational logic 39 is provided to handle the special case in which at least one of the operands is zero. The separate handling of this special case allows the barrel shifter 32 to perform addition modulo  $m_i-1$ , rather than modulo  $m_i$ . As in the adder 10 of Figure 1(a), a static pipeline register 14 stores the resulting product for downstream processing.

While offering such advantageous characteristics and a very low delay-power product, conventional RNS arithmetic circuits are not testable. In particular, conventional RNS arithmetic circuits do not include simple test circuitry to allow verification of circuit functionality and timing. The input-to-output delay is one of the critical timing values of an RNS arithmetic circuit that must be verified to be within specification. Such timing verification must be provided before RNS arithmetic circuits can be practically used for digital signal processing in actual products such as hard disk drive read channels, wireless telecommunication integrated circuits, and image processing integrated circuits.

#### SUMMARY OF THE INVENTION

It is an object of the present invention to provide testable arithmetic circuits for use with the Residue Number System (RNS).

Another object of the present invention is to provide RNS arithmetic circuits that have simple circuitry for performing built-in self testing of input-to-output delay.

One embodiment of the present invention provides an arithmetic circuit for use with an RNS. The arithmetic circuit includes an arithmetic core having an output and at least two inputs, test circuitry coupled to the arithmetic core, and logic circuitry coupled to the output of the arithmetic core. The arithmetic core performs an RNS arithmetic operation, and the test circuitry induces oscillation at the output of the arithmetic core



**EXPRESS MAIL LABEL NO.: EL563155563US**

during testing. The logic circuitry produces a pass/fail signal based on whether the oscillation frequency of the arithmetic core is at least equal to a minimum threshold value. In a preferred embodiment, the logic circuitry includes a counter that counts oscillations of the output of the arithmetic core during testing, and a comparator that  
5 compares the output of the counter after a predetermined test period with the minimum threshold value.

Another embodiment of the present invention provides a method for testing the propagation delay of an RNS arithmetic circuit having an arithmetic core that performs an RNS arithmetic operation. According to the method, the output of the arithmetic core is  
10 fed back to one of the inputs of the arithmetic core, and a constant is provided to another input of the arithmetic core so as to induce oscillation at the output of the arithmetic core. A pass/fail signal is produced based on whether the oscillation frequency of the arithmetic core is at least equal to a minimum threshold value. In one preferred method, the pass/fail signal is produced by counting oscillations of the output of the arithmetic core  
15 during a predetermined time period, and comparing the counted oscillations with the minimum threshold value to determine a pass or fail condition.

Other objects, features, and advantages of the present invention will become apparent from the following detailed description. It should be understood, however, that the detailed description and specific examples, while indicating preferred embodiments of  
20 the present invention, are given by way of illustration only and various modifications may naturally be performed without deviating from the present invention.

**BRIEF DESCRIPTION OF THE DRAWINGS**

Figure 1(a) is a diagram showing a conventional OHRNS modulo  $m_i$  adder;  
25 Figure 1(b) is a circuit diagram showing a barrel shifter for  $m_i=5$ ;  
Figure 2 is a block diagram showing a conventional OHRNS modulo  $m_i$  subtractor;

**EXPRESS MAIL LABEL NO.: EL563155563US**

Figure 3 is a block diagram showing a conventional OHRNS modulo  $m_i$  multiplier;

Figure 4 is a block diagram showing a testable OHRNS arithmetic circuit according to a preferred embodiment of the present invention;

5        Figure 5 is a block diagram showing a testable OHRNS modulo  $m_i$  adder according to one embodiment of the present invention;

Figure 6 is a circuit diagram showing an exemplary embodiment for the clocked latch of the OHRNS adder of Figure 5; and

10        Figure 7 is a block diagram showing a testable OHRNS modulo  $m_i$  multiplier according to another embodiment of the present invention.

**DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS**

Preferred embodiments of the present invention will be described in detail hereinbelow with reference to the attached drawings.

15        The core circuits used to perform OHRNS arithmetic operations have the advantageous property that input-to-output timing is identical for all inputs and outputs. The present invention takes advantage of this property to enable verification of the timing of the circuit with simple built-in self test circuitry. In preferred embodiments, the input-to-output delay of an OHRNS arithmetic circuit is tested using Oscillation Built-In Self  
20        Test (OBIST). More specifically, the circuit is made to oscillate by feeding the output back to the input, and the frequency of oscillation of the circuit is measured. Because the frequency of oscillation is inversely proportional to the input-to-output delay of the circuit, the measured frequency can be used to ascertain whether or not the delay of the circuit is within specification. (A general explanation of OBIST can be found in K. Arabi  
25        et al., "Oscillation Built-In Self-Test (OBIST) Scheme for Functional and Structural Testing of Analog and Mixed-Signal Integrated Circuits," Proceedings of the IEEE

**EXPRESS MAIL LABEL NO.: EL563155563US**

International Test Conference, Washington, D.C. (1997), pp. 786-795, which is herein incorporated by reference.)

Figure 4 shows an OHRNS modulo  $m_i$  arithmetic circuit with built-in delay self test in accordance with a preferred embodiment of the present invention. As shown, the circuit includes an OHRNS arithmetic core 40, a counter 48, and test logic 50. The arithmetic core 40 is a basic circuit for performing an OHRNS modulo  $m_i$  arithmetic operation such as addition, subtraction, multiplication, or scaling. Additionally, the circuit includes transmission gates 42, 44, and 46 that selectively provide feedback, and tristate buffers 52, 54, 56, and 58 that isolate the circuit during testing. The transmission gates can be implemented using either one or two MOS pass transistors and are controlled by a test enable signal. In preferred embodiments, the OHRNS arithmetic circuit of the present invention is incorporated into an integrated circuit device.

The operation of the OHRNS arithmetic circuit of Figure 4 will now be explained. During normal operation, the test enable signal is held in the inactive state (e.g., low). This causes the transmission gates 42, 44, and 46 to be open and the tristate buffers 52, 54, 56, and 58 to be enabled. Thus, feedback is disabled and the inputs and outputs of the arithmetic core 40 of the circuit are coupled to the other circuitry of the integrated circuit device to provide the desired operation. In this state, the arithmetic core 40 performs its particular OHRNS operation and the result is supplied to the downstream circuitry in the usual manner.

During testing, the test enable signal is changed to the active state (e.g., high). This disables the tristate buffers and closes the transmission gates to induce oscillation. More specifically, the active test enable signal causes the tristate buffers to go into a high impedance state so as to isolate the inputs and outputs of the arithmetic core 40 from the other circuitry of the integrated circuit device. Additionally, the active test enable signal causes the first transmission gate 42 to feed the  $m$  output lines of the arithmetic core 40 back to one of the operand inputs, and the second transmission gate 44 to transfer a one-

**EXPRESS MAIL LABEL NO.: EL563155563US**

hot encoded constant  $k$  that will cause oscillation of the output to the other operand input of the arithmetic core 40.

For example, if the arithmetic core 40 is a OHRNS adder, the constant  $k$  is preferably set equal to 1 so as to form an analog version of a numerically controlled oscillator (NCO) with a phase increment value of 1 and a modulus of  $m_i$ . Similarly, if the arithmetic core 40 is a OHRNS multiplier, the constant  $k$  is set equal to any value other than 0 or 1 so as to form an analog "multiply-accumulate circuit" (MAC) whose output sequence is the nonzero integers modulo  $m_i$ . Furthermore, if the arithmetic core 40 is the type of circuit that has a gating input  $G$  for activating latches that are provided on the output lines, the active test enable signal is supplied to the gating input  $G$  through the third transmission gate 44 in order to activate the output latches for the duration of the testing period.

The frequency of oscillation  $f$  of the resulting oscillatory signal is measured by coupling one of the output lines of the arithmetic core 40 to the clock input of the counter 48. In the case of an OHRNS adder, the frequency of oscillation  $f$  of the NCO (measured at any one of the output lines) depends only on the modulus and the propagation delay  $t_d$  between the input and output of the arithmetic core 40 as shown by the following equation.

$$f = 1 / (m_i \times t_d)$$

In the case of an OHRNS multiplier, the frequency of oscillation  $f$  of the MAC also depends only on the modulus and the propagation delay  $t_d$  between the input and output of the arithmetic core 40 as shown by the following equation.

$$f = 1 / ((m_i - 1) \times t_d)$$

**EXPRESS MAIL LABEL NO.: EL563155563US**

During testing, the counter 48 is enabled by the active test enable signal and counts the oscillations of the output of the arithmetic core. The output of the counter 48 is supplied to the test logic 50. The number of oscillations during a fixed period of time is directly proportional to the frequency of oscillation  $f$  and inversely proportional to the propagation delay  $t_d$ . Thus, calculation or measurement of test cases can be used to determine the minimum frequency of oscillation  $f_{\min}$  that corresponds to the highest acceptable propagation delay of the circuit. The test logic 50 compares the selected minimum frequency of oscillation  $f_{\min}$  with the output of the counter 48 after a predetermined test time  $T$  has elapsed.

10 If the number of oscillations during the test period  $T$  (as indicated by the output of the counter) is less than the lower limit threshold given by the minimum frequency of oscillation  $f_{\min}$ , the test logic 50 outputs a fail signal. Conversely, if the output of the counter 48 at least equals the selected threshold value  $f_{\min}$ , the test logic 50 outputs a pass signal. The pass/fail signal output by the test logic of the arithmetic circuit can be  
15 directly or indirectly provided to an external device. For example, the pass fail signal can be directly provided to a dedicated pin of the integrated circuit, stored in a register and later scanned out, or supplied to further logic circuitry or a controller that provides a single external pass/fail signal for all of the circuitry of the integrated circuit device. When the test enable signal returns to the inactive state, normal circuit operation is  
20 resumed and the counter 48 is reset.

Figure 5 shows a testable OHRNS modulo  $m_i$  adder in accordance with one embodiment of the present invention. In this exemplary embodiment, the adder 60 includes a barrel shifter 62 and a dynamic storage unit 64. The barrel shifter 62 computes the sum of the two operands in the manner described above with reference to Figures 1(a)  
25 and 1(b). The dynamic storage unit 64 includes two cascaded inverter stages 66 and 67 for each output line of the barrel shifter 62. The cascaded inverter stages 66 and 67

**EXPRESS MAIL LABEL NO.: EL563155563US**

dynamically latch the output of the barrel shifter 62 for downstream circuits by using a clocked inverter 66 as the first inverter in the cascade.

Additionally, isolation buffers 63 are provided on the input and output lines of the adder, and transmission gates 65 are used to induce oscillation. As in the circuit of Figure 4, a test enable signal is asserted to isolate the inputs and outputs, provide feedback through the transmission gates 65, and to enable a counter 61. During testing, the test enable signal is also provided to the clocked inverters of the dynamic storage unit 64 through a transmission gate. After a predetermined test time T has elapsed, test logic 70 compares the output of the counter with a lower limit threshold and produces a pass/fail signal. When the test enable signal is not asserted, the transmission gates are opened to disable feedback, and the OHRNS adder operates in the normal manner.

A preferred embodiment for the clocked inverters of Figure 5 is shown in Figure 6. The clocked inverter has two PMOS transistors 72 and 74 and two NMOS transistors 76 and 78 arranged in series between the supply voltage Vdd and ground. The gates of the outer PMOS and NMOS transistors 72 and 78 receive the output of the barrel shifter, and the inner PMOS and NMOS transistors 74 and 76 receive a clock signal  $\phi$  in inverted and non-inverted form, respectively. The connection point of the inner PMOS and NMOS transistors 74 and 76 provides the output OUT of the clocked inverter. When the clock signal  $\phi$  is high, the clocked inverter operates as a standard CMOS inverter. On the other hand, when the clock signal  $\phi$  is low, the output of the clocked inverter is tristated so as to cause any charge on the output node of the clocked inverter 66 to be trapped. Therefore, as long as the clock period is relatively short, the output of the second inverter 67 is held substantially steady.

Additionally, in the preferred embodiment, a pull-up transistor 79 controlled by the output OUT is connected between the supply voltage Vdd and the input IN of the latch. When pass transistors are used to implement the barrel shifter 62, high level output

**EXPRESS MAIL LABEL NO.: EL563155563US**

5 signals from the barrel shifter experience voltage degradation (i.e., the output signal does not swing fully to the high rail). Such degraded signal levels cause static power dissipation in downstream circuitry, and thus increase power consumption. However, output level restoration can be used to prevent such leakage power dissipation in the downstream circuitry. The pull-up transistor 79 is used to perform such voltage level restoration at the output of the barrel shifter. In particular, when the input to the clocked inverter goes to the degraded high level that is output by the barrel shifter, the low level output of the inverter turns on the pull-up transistor 79 to couple the input to the supply voltage Vdd (i.e., the desired high level voltage).

10 Figure 7 shows a testable OHRNS modulo  $m_i$  multiplier according to one embodiment of the present invention. As shown, the multiplier 80 uses signal transpositions 84, 86, and 88 on the input and output lines to compute the indices and anti-indices, and a barrel shifter 82 to add the indices. A small amount of combinational logic 89 is used to handle the special case in which at least one of the operands is zero-valued. The separate handling of this special case allows the barrel shifter 82 to perform addition modulo  $m_i-1$ , rather than modulo  $m_i$ . In this exemplary embodiment, a dynamic storage unit 64 stores the resulting product for downstream processing.

15 Additionally, isolation buffers 90 are provided on the input and output lines, and transmission gates 92 are used to induce oscillation. As in the circuit of Figure 4, a test enable signal is asserted to isolate the inputs and outputs, provide feedback through the transmission gates 92, and to enable a counter 94. During testing, the test enable signal is also provided to the clock input of the dynamic storage unit 64 through a transmission gate. After a predetermined test time T has elapsed, the test logic 96 compares the output of the counter 94 with a lower limit threshold and produces a pass/fail signal. When the test enable signal is not asserted, the transmission gates are opened to disable feedback, and the OHRNS multiplier operates in the normal manner.

**EXPRESS MAIL LABEL NO.: EL563155563US**

Accordingly, the present invention provides testable arithmetic circuits for use with the Residue Number System. During testing, the arithmetic circuit is isolated from other circuitry and made to oscillate by feeding the output back to the input. The frequency of oscillation of the circuit is measured and used to determine whether or not the propagation delay of the circuit is within specification. Because timing verification is possible, the RNS arithmetic circuits of the present invention can be used in practical digital signal processing devices.

The embodiments of the present invention described above relate to specific CMOS circuit implementations and the use of "one-hot" encoding. However, the arithmetic circuits of the present invention could also be implemented using other integrated circuit technologies and other encoding schemes (e.g., a "one-cold" encoding scheme). Similarly, signal transposition may be achieved in various manners (e.g., through a simple renaming of the lines). Additionally, other design choices, such as the number and values of moduli in the RNS, the physical size and layout of the circuit elements, and the timing of the clock signals could easily be adapted by one of ordinary skill in the art. Furthermore, embodiments of the present invention may not include all of the features described above. For example, pass transistor-based barrel shifters, dynamic latching, and signal level restoration may not be included in all embodiments.

While there has been illustrated and described what are presently considered to be the preferred embodiments of the present invention, it will be understood by those skilled in the art that various other modifications may be made, and equivalents may be substituted, without departing from the true scope of the present invention. Additionally, many modifications may be made to adapt a particular situation to the teachings of the present invention without departing from the central inventive concept described herein. Therefore, it is intended that the present invention not be limited to the particular embodiments disclosed, but that the invention include all embodiments falling within the scope of the appended claims.